EXHIBIT 3

APPENDIX B

APPENDIX B: IEEE Standards and Protocols

1. I have reviewed Arista's responses, including supplemental responses to Cisco's Interrogatory No. 10 and incorporate the identification of IEEE publications and other industry-standard documents cited in those responses for the disputed CLI commands.

A. IEEE Std 802.1X ("DOT1X")

2. IEEE Standard 802.1X, also referred to as "dot1x," is an IEEE standard for port-based network access control and is part of the IEEE 802.1 group of networking protocols. IEEE 802.1X was originally published as a supplement to IEEE Standard 802.1D-1998, but thereafter has been published as a standalone standard, including IEEE Standard 802.1X-2001, IEEE Standard 802.1X-2004, and IEEE Standard 802.1X-2010.

3. IEEE 802.1X provides an authentication mechanism to devices wishing to attach to a LAN or WLAN, and involves three entities that are defined in the standard: (1) a supplicant, (2) an authenticator, and (3) an authentication server. The standard also defines a Port Access Entity, or PAE, which is the protocol entity associated with a port.

4. The following CLI commands in this litigation provide functionality relating to the IEEE Standard 802.1X (shown in chronological order based on Cisco's purported "earliest document date" for each alleged command):

Disputed "Command"	Earliest Document Date	Additional Opinions
show dot1x	May 20, 2000	IEEE 802.1x-2001 (2001) uses the shorthand "dot1x" as seen in Table 10-1 of the standard.
dot1x port-control	May 21, 2001	IEEE 802.1x-2001 § 8.5.2.2 ("Global variables") defines a "portControl" variable.

dot1x reauthentication	May 21, 2001	IEEE 802.1x-2001 § 5.1 ("Static conformance requirements") discusses "reauthentication." This is also discussed in §§ 8.3.3, 8.4.2.1, and 8.4.4.
dot1x system-auth-control	May 21, 2001	IEEE 802.1x-2001 § 9.6.1.1.3 ("Outputs"): "SystemAuthControl. The value of the SystemAuthControl parameter (6.3) for the System. This parameter can take the values Enabled and Disabled."
dot1x timeout quiet-period	May 22, 2001	IEEE 802.1x-2001 § 8.5.2.1 ("Timers"): "quietWhile. A timer used by the Authenticator state machine to define periods of time during which it will not attempt to acquire a Supplicant. The initial value of this timer is quietPeriod." IEEE 802.1x-2001 § 8.5.4.1.2 ("Constants"): "quietPeriod. The initialization value used for the quietWhile timer. Its default value is 60 s; it can be set by management to any value in the range from 0 to 65 535 s."
dot1x timeout tx-period	May 22, 2001	IEEE 802.1x-2001 § 8.5.2.1 ("Timers"): "txWhen. A timer used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted. The initial value of this timer is txPeriod." Also, IEEE 802.1x-2001 § 8.5.4.1.2 ("Constants"): "txPeriod. The initialization value used for the txWhen timer. Its default value is 30

		s; it can be set by management to any value in the range from 1 to 65 535 s."
dot1x timeout reauth-period	May 24, 2001	IEEE 802.1x-2001 § 8.4.4 ("Timing out authorization state information"): "Authenticator PAEs can time out the authorization state information on a periodic basis by means of the Reauthentication Timer State Machine (8.5.7). The time period for such timeouts is reAuthPeriod seconds since the last time that the authorization state was confirmed. The state variable reAuthEnabled controls whether periodic reauthentication takes place."
show dot1x statistics	May 24, 2001	IEEE 802.1x-2001 § 9.4.2 ("Authenticator Statistics"): "The Authenticator Statistics managed object models the operations that modify, or enquire about, the statistics associated with the operation of the Authenticator. There is a single Authenticator Statistics managed object for each Port that supports Authenticator functionality." Also see §§ 9.4.4 and 9.5.2.
dot1x pae authenticator	February 3, 2004	IEEE 802.1x-2001 § 6.2 ("Port access entity") discusses the "Authenticator PAE". This is also discussed in §§ 9.4 and 10.4.3.
dot1x max-reauth-req	June 30, 2004	IEEE 802.1x-2001 § 8.5.4.1.2 ("Constants"): "reAuthMax. The number of reauthentication attempts

		that are permitted before the Port becomes Unauthorized. The default value of this constant is 2." This is also discussed in §§ 8.5.4.5 and 8.5.8.7.
show dot1x all summary	August 4, 2005	"show" commands come from prior legacy CLIs, as discussed elsewhere in this Report.
aaa accounting dot1x	March 29, 2006	The constituent command words are addressed elsewhere in this table, as well as in the "AAA" section of this Appendix.

B. Link Aggregation Control Protocol ("LACP")

5. The Link Aggregation Control Protocol, or LACP, was initially defined by IEEE Standard 802.3AD. Generally speaking, link aggregation refers to the combination (or aggregation) of multiple network connections in parallel to both to increase throughput beyond what a single connection might permit, and to provide redundancy in case one of the multiple links fails.

6. In the late 1990s, the IEEE 802.3 Working Group began work on creating a standard and interoperable link aggregation protocol to replace the various vendor-specific link aggregation methods introduced by each manufacturer in the mid-1990s. The IEEE's work resulted in IEEE Standard 802.3AD-2000 (published in 2000), which describes an interoperable and standardized link-layer protocol known as LACP. It was later incorporated into IEEE Standard 802.3 as clause 43 of IEEE Standard 802.3-2005, and thereafter published as IEEE Standard 802.1AX-2008 (the IEEE transferred LACP to the 802.1 group in 2008).

7. As described by the IEEE specification, LACP provides a method to control the bundling of physical network links to form a single logical channel.

8. The following CLI commands in this litigation provide functionality relating to LACP (shown in chronological order based on Cisco's purported "earliest document date" for each alleged command):

Disputed "Command"	Earliest Document Date	Additional Opinions
show lacp neighbor	May 7, 2001	"show" commands come from prior legacy CLIs, as discussed elsewhere in this Report. IEEE Std 802.3 (2000) disclosed "LACP" at Section 43.4 ("Link Aggregation Control Protocol"): "The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner." IEEE Std 802.3 (2000) provides an example of aggregation with a "neighbor" at Section 43C.7: "This is equivalent to each port being able to aggregate with either neighbor, understanding the ports to be arranged in a circle."

lacp port-priority	May 7, 2001	IEEE Std 802.3 (2000 edition) at § 43.3.4 ("Port Identification"): "Link Aggregation Control uses a Port Identifier, comprising the concatenation of a Port Priority and a Port Number, to identify the port. Port Numbers (and hence, Port Identifiers) shall be uniquely assigned within a System. Port Number 0 shall not be assigned to any port."
lacp system-priority	May 7, 2001	IEEE Std 802.3 (2000) disclosed "LACP" as well as a "System Priority" parameter at Section 43.4.2: "The globally unique identifier used to identify a System shall be the concatenation of a globally administered individual MAC address and the System Priority. … The two most significant octets of the System Identifier comprise the System Priority. The System Priority value is taken to be an unsigned binary number; the most significant octet of the System Priority forms the most significant octet of the System Identifier." Also see IEEE Std 802.3 (2000 edition) at § 43C.3 ("Every link between systems operating LACP is assigned a unique priority. This priority comprises (in priority order) the System Priority, System ID, Port Priority, and Port Number of the higher-priority system. In priority comparisons, numerically lower values have higher priority.")

show lacp counters	May 7, 2001	IEEE Std 802.3 (2000) discusses the use of counters, including for Link Aggregation at Sections 5.2.1 and 30.7: "[5.2.1] All counters defined in this specification are assumed to be wraparound counters. Wraparound counters are those that automatically go from their maximum value (or final value) to zero and continue to operate. These unsigned counters do not provide for any explicit means to return them to their minimum (zero), i.e., reset. Because of their nature, wraparound counters should be read frequently enough to avoid loss of information."
lacp rate	October 18, 2005	IEEE Std 802.3 (2000) discusses different transmission rates for LACP at Section 43.4.13 ("Periodic Transmission machine"): "Transmissions occur at a rate determined by the Partner; this rate is linked to the speed at which the Partner will time out received information. The state machine has four states. They are as follows: … FAST_PERIODIC. While in this state, periodic transmissions are enabled at a fast transmission rate. … SLOW_PERIODIC. While in this state, periodic transmissions are enabled at a slow transmission rate."

show lacp interface	October 30, 2007	IEEE Std 802.3 (2000) discusses LACP interfaces at Sections 30C.5 and 30C.5.1: "[30C.5.a] It is assumed that a system implementing this MIB will also implement (at least) the 'system' group defined in MIB-II defined in RFC 1213 and the 'interfaces' group defined in RFC 2233."

C. Link Layer Discovery Protocol ("LLDP")

9. The Link Layer Discovery Protocol, or LLDP, is defined by IEEE Standard 802.1AB. After several years of development, LLDP was formally defined as IEEE Standard 802.1AB-2005 (published in May 2005).

10. Unlike vendor-specific discovery protocols, including Cisco Discovery Protocol (CDP), Extreme Discovery Protocol, Foundry Discovery Protocol (FDP), Nortel Discovery Protocol (also known as SONMP), and Microsoft's Link Layer Topology Discovery (LLTD), LLDP is a vendor-neutral layer 2 protocol that is used used by network devices to advertise their identity, capabilities, and neighbors on the network.

11. As confirmed by former Cisco engineer Devadas Patil at his deposition, the vast majority of command terms--if not all of them--were taken either from pre-existing CLI command syntaxes (*e.g.*, use of "show" commands or re-use of the command set for CDP), or from terms taken directly from the LLDP industry standard.

12. The following CLI commands in this litigation provide functionality relating to LLDP (shown in chronological order based on Cisco's purported "earliest document date" for each alleged command):

Disputed "Command"	Earliest Document Date	Additional Opinions
clear lldp counters	November 16, 2005	"clear" commands come from prior legacy CLIs, as discussed elsewhere in this Report. IEEE Std 802.1AB-2005 (May 2005) disclosed LLDP in Section 1: "The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802® LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to the IEEE 802 LAN required by those management entity or entities."
clear lldp table	November 16, 2005	IEEE Std 802.1AB-2005 (May 2005) defines several objects that include "tables" as part of the LLDP MIB in Section 12.2.
lldp holdtime	November 16, 2005	IEEE Std 802.1AB-2005 (May 2005) disclosed a similar parameter called "msgTxHold" in Sections 10.1.1 and 10.5.3.3.
lldp reinit	November 16, 2005	IEEE Std 802.1AB-2005 (May 2005) disclosed a similar parameter called "reinitDelay" in Section 10.1.1.
lldp run	November 16, 2005	IEEE Std 802.1AB-2005 § 3.1 ("Definitions") uses "run" in the same way that the command uses

		this term:.
lldp timer	November 16, 2005	IEEE Std 802.1AB-2005 (May 2005) describes several timers, including the one to which this command pertains at Section 10.5.3 ("Timers"): "The timer used for LLDP state machines decrements countdown counters that keep time values for the all objects in the resident station's LLDP MIB." Also see IEEE Std 802.1AB-2005 § 10.5.3.3 ("Transmit state machine timing parameters"): "The following timing counters are used in conjunction with the timers defined in 10.5.3.1: … msgTxInterval: This parameter indicates the interval at which LLDP frames are transmitted on behalf of this LLDP agent. The recommended default value for msgTxInterval is 30 seconds." This command refers in particular to the msgTxInterval PDU transmission rate.
lldp tlv-select	November 16, 2005	IEEE Std 802.1AB-2005 (May 2005) describes TLV selection management in Sections 7.5 ("TLV section") and 11.2.2 ("TLV selection management").
show lldp	November 16, 2005	"show" commands come from prior legacy CLIs, as discussed elsewhere in this Report.
show lldp neighbors	November 16, 2005	IEEE Std 802.1AB-2005 (May 2005)

		discusses "neighbors" in the context of LLDP at Section 11.2.4. In addition, the standard defines a variable called "tooManyNeighbors" in Section 10.5.5.1. The use of "neighbors" in the LLDP standard--as it is used in all disputed commands--is consistent with industry customary meaning.
show lldp traffic	November 16, 2005	The use of "traffic" in this command is the same as was known and understood in the industry as of 2005, which--generally speaking--is the amount of data traversing the network at a given point of time.
lldp receive	February 1, 2006	IEEE Std 802.1AB-2005 (May 2005) describes LLDP operational modes ("transmit" or "receive") at Section 7.1: "LLDP is a one way protocol. An LLDP agent can transmit information about the capabilities and current status of the system associated with its MSAP identifier. The LLDP agent can also receive information about the capabilities and current status of the system associated with a remote MSAP identifier."
lldp transmit	February 1, 2006	See immediately above.

D. Precision Time Protocol ("PTP")

13. The Precision Time Protocol, or PTP, was originally defined in the IEEE

Standard 1588-2002, which is titled "Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems" and published in 2002. A revised PTP standard, version 2, was published as IEEE Standard 1588-2008 in 2008, and featured improved accuracy, precision, and robustness.

14. PTP defined in IEEE Standard 1588-2008 is a standardized protocol used to synchronize clocks throughout a network, and achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems. It performs functionality similar to the IETF-defined NTP, or Network Time Protocol, which is a different standardized protocol discussed elsewhere in this Report.

15. I have reviewed the deposition testimony of Tong Liu, the former Cisco engineer who supposedly authored several of these disputed PTP commands, and confirmed that Ms. Liu based the vast majority of the command terms on the terminology used in the PTP standard.

16. The following CLI commands in this litigation provide functionality relating to PTP (shown in chronological order based on Cisco's purported "earliest document date" for each alleged command):

Disputed "Command"	Earliest Document Date	Additional Opinions
ptp priority1	June 25, 2008	IEEE Std 1588-2008 (Mar. 2008) disclosed and defined the acronym "ptp" in Section 3.1.28: "Precision Time Protocol (PTP): The protocol defined by IEEE Std 1588-2008. As an adjective, it indicates that the modified noun is specified in or interpreted in the context of IEEE Std 1588-2008."

		The term "priority1" comes directly from IEEE Std 1588-2008 § 6.6.2.3 ("Best master clock algorithm"): "... priority1: A user configurable designation that a clock belongs to an ordered set of clocks from which a master is selected"
ptp priority2	June 25, 2008	The term "priority2" comes directly from IEEE Std 1588-2008 § 6.6.2.3 ("Best master clock algorithm"): "... priority2: A user configurable designation that provides finer grained ordering among otherwise equivalent clocks"
ptp sync interval	June 25, 2008	The term "sync interval" comes directly from IEEE Std 1588-2008 § 7.7.2.3 ("Sync (multicast) message transmission interval"): "The portDS.logSyncInterval shall specify the mean time interval between successive Sync messages, i.e., the syncInterval, when transmitted as multicast messages."). Also see Table 40 in the standard.
show ptp clock	June 25, 2008	"show" commands come from prior legacy CLIs, as discussed elsewhere in this Report. The term "clock" comes directly from IEEE Std 1588-2008 § 3.1.4: "clock: A node participating in the Precision Time Protocol (PTP) that is capable of providing a measurement of the passage of time since a defined epoch."

show ptp parent	June 25, 2008	The term "clock" comes directly from IEEE Std 1588-2008 § 3.1.23: "3.1.23 parent clock: The master clock to which a clock is synchronized." The term "parent" slone is also used in the IEEE standard to refer to the parent clock, as discussed in the deposition of Tong Liu.
ptp domain	July 23, 2009	The term "clock" comes directly from IEEE Std 1588-2008 § 3.1.7: "domain: A logical grouping of clocks that synchronize to each other using the protocol, but that are not necessarily synchronized to clocks in another domain."
show ptp time-property	October 12, 2009	IEEE Std 1588-2008 (Mar. 2008) discloses a "time properties" data set at Section 15.5.3.6.1.

E. Spanning-Tree Protocol ("STP") & Related Protocols (RSTP and MSTP)

17. The Spanning Tree Protocol, or STP, was initially defined by IEEE Standard 802.1D in 1990, which was extended by the IEEE in 1998 and 2004. STP serves two purposes: (1) it prevents problems caused by loops on a network; and (2) when redundant loops are planned on a network, STP deals with remediation of network changes or failures.

18. The IEEE also introduced the Rapid Spanning Tree Protocol, or RSTP, in 2001 as IEEE Standard 802.1W. RSTP provides faster spanning-tree convergence after a topology change, and is backwards-compatible with STP.

19. The Multiple Spanning Tree Protocol, or MSTP, was first specified in IEEE

Standard 802.1S and later merged into IEEE 802.1Q-2005. MSTP defines an extension to RSTP to improve the usefulness of virtual LANs (VLANs) by configuring a separate Spanning Tree for each VLAN group and blocking all but one possible alternate path within each Spanning Tree.

20. Much of the STP, RSTP, and MSTP functionality has been incorporated into IEEE 802.1Q-2014.

21. The following CLI commands in this litigation provide functionality relating to STP, RSTP, and/or MSTP (shown in chronological order based on Cisco's purported "earliest document date" for each alleged command):

Disputed "Command"	Earliest Document Date	Additional Opinions
show spanning-tree	November 2, 1998	"show" commands come from prior legacy CLIs, as discussed elsewhere in this Report. The term "spanning-tree" refers to Spanning Tree Protocol, defined in IEEE Std 802.1D-1990 at Section 4.
spanning-tree cost	January 4, 1999	The term "cost" refers Path Cost, which defines a value of an interface / port when STP algorithm is calculated. Path Cost is defined in the IEEE Std 802.1D (1990) at Section 6.8.2.3.
spanning-tree port-priority	January 4, 1999	The term "port-priority" refers to Port Priority variable, defined in the IEEE Std 802.1D (1990) at Section 6.8.2.3.
spanning-tree vlan	January 4, 1999	This command involves configuring STP parameters on a particular vlan

		(PVSTP). VLANs are discussed elsewhere in this Appendix.
show spanning-tree interface	February 24, 2000	The term "interface" in this context refers to the spanning tree attributes associated with a particular port. Port States and parameters are defined in IEEE Std 802.1D-1990 (see Sections 4.4 and 4.6.6) and subsequent versions of the standard.
spanning-tree mode	July 17, 2000	The term "mode" refers to the ability to select the type of STP protocol to operate (contrast STP vs. RSTP vs. MST). IEEE Std 802.1w-2001 at Section 7.16.1 refers to operating a switch in compatibility mode to permit the coexistence of several types of STP protocols.
spanning-tree guard	May 16, 2001	The constituent command words are addressed elsewhere in this table and Appendix. This command relates to security and stability functionality for STP.
spanning-tree mst configuration	July 23, 2001	The constituent command words are addressed elsewhere in this table and Appendix.
spanning-tree link-type	September 4, 2001	The term "link-type" in this context refers to the type of port connectivity (*i.e.* point-to-point vs shared) while implementing RSTP. This is described in IEEE Std 802.1D (2004) § 17.12.
spanning-tree loopguard	September 26, 2001	The constituent command words are

default		addressed elsewhere in this table and Appendix. This command relates to security and stability functionality for STP.
spanning-tree bpdufilter	October 31, 2001	The constituent command words are addressed elsewhere in this table and Appendix. This command relates to security and stability functionality for STP. The acronym "bpdu" is a well-known industry-standard term used in the IEEE standards that means "bridge protocol data unit," which is a frame used by all spanning-tree protocols. BDPUs are transmitted across a local area network to detect loops in network topologies. This command and other commands relating to security and stability are intended to protect an interface in a spanning-tree topology from BPDUs generated from other devices. This functionality is commonly supported by many vendors.
spanning-tree bpduguard	October 31, 2001	The constituent command words are addressed elsewhere in this table and Appendix. This command relates to security and stability functionality for STP.
spanning-tree portfast bpdufilter default	October 31, 2001	The constituent command words are addressed elsewhere in this table and

		Appendix. This command relates to security and stability functionality for STP.
spanning-tree portfast bpduguard default	October 31, 2001	The constituent command words are addressed elsewhere in this table and Appendix. This command relates to security and stability functionality for STP.
clear spanning-tree counters	April 10, 2002	"clear" commands come from prior legacy CLIs, as discussed elsewhere in this Report.
show spanning-tree mst	April 10, 2002	The term "mst" in this context refers to the Multiple Spanning Tree version of Spanning Tree Protocol, defined in IEEE Std 802.1Q, 2003 Edition (and mentioned above). IEEE Std 802.1Q (2003) § 13 uses the acronym "MST" for "Multiple Spanning Tree."
show spanning-tree mst configuration	April 10, 2002	The term "configuration" in this context refers to the parameters of the MST region currently operating on this particular platform. IEEE Std 802.1Q (2003) § 13.2 discusses these "configuration parameters."
show spanning-tree mst interface	April 10, 2002	The term "interface" in this context refers to the MST specific parameters currently available at a particular interface. Port States and parameters are defined in IEEE Std

		802.1Q, 2003 Edition (for example, in Section 13.12) and subsequent versions of the standard.
spanning-tree transmit hold-count	February 18, 2005	The term "transmit hold-count" refers to TxHoldCount, a variable of the Port Transmit State Machine, defined in IEEE Std 802.1W (2001) at Section 17.27. IEEE Std 802.1D (2004) § 14.8.1 also discusses the "TxHoldCount" variable.
show spanning-tree root	November 2, 2005	The term "root" refers to the information of the Switch selected as the Designated Root bridge. Root bridge selection process is defined in IEEE Std 802.1D (1990) at Section 4.6.8.
show spanning-tree blockedports	December 11, 2006	The term "blockedports" refers to the interfaces/ports that are in Blocking State after Spanning Tree Algorithm removes loops thru redundant links. This is described in IEEE Std 802.1D-1990 at in Sections 4.3 and Section 4.4 (discussing the "blocking" state of a Port).
show spanning-tree bridge	December 11, 2006	The term "bridge" in this context refers to the information about the spanning tree instance running on the device itself. The term "bridge" is a well-known networking term to represent a Layer 2 / Ethernet device.

spanning-tree bridge assurance	October 16, 2007	

F. Virtual Local Area Network ("VLAN") and Private Virtual LAN ("PVLAN")

22. A local area network, or LAN, provides the nodes connected to it with direct (Layer 2) access to one another. It is usually comprised of one or more Ethernet switches. Computers on different LANs talk to each other using Layer 3 (IP), via a router. A virtual LAN ("VLAN") abstracts the idea of the LAN. A VLAN might comprise a subset of the ports on a single switch or subsets of ports on multiple switches. By default, systems on one VLAN don't see the traffic associated with systems on other VLANs on the same network. VLANs allow network administrators to partition their networks to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure.

23. IEEE Std 802.1Q-2005 (also called "dot1q" in the industry) is the most commonly used standard defining VLANs on an Ethernet network. However, Virtual LANs have been discussed in earlier publications, such as RFC 2674 (Aug. 1999) ("Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions"). IEEE Std 802.3ac-1998 also addressed VLANS as specified in IEEE 802.1Q.

24. Private VLAN ("PVLAN") is a technique in computer networking where a VLAN contains switch ports that are restricted such that they can only communicate with a given "uplink". The restricted ports are called "private ports." Each private VLAN typically contains many private ports, and a single uplink. The uplink will typically be a port (or link aggregation group) connected to a router, firewall, server, provider network, or similar central

resource. As a result, direct peer-to-peer traffic between peers through the switch is blocked, and any such communication must go through the uplink. While private VLANs provide isolation between peers at the data link layer, communication at higher layers may still be possible depending on further network configuration.

25. The following CLI commands in this litigation provide functionality relating to VLANs (shown in chronological order based on Cisco's purported "earliest document date" for each alleged command):

Disputed "Command"	Earliest Document Date	Additional Opinions
interface vlan	January 15, 1997	The acronym "vlan" is a commonly used term for virtual lan, and is a defined "Abbreviation" in Section 4 of the IEEE Std. 802.1Q-2005. The "interface" command keyword is a commonly used keyword and term that refers to the various interfaces on a switch or router, and is used by many vendors in the industry.
show vlan	July 25, 1997	"show" commands come from prior legacy CLIs, as discussed elsewhere in this Report.
switchport access vlan	April 13, 1998	IEEE Std. 802.1Q § D.1.2 discusses "Access Links" in the VLAN context.
switchport trunk allowed vlan	April 13, 1998	IEEE Std. 802.1Q § D.1.1 discusses "Trunk Links" in the VLAN context.
switchport trunk native vlan	April 13, 1998	The term "native" in this context refers to an untagged vlan, which is defined in IEEE Std. 802.1Q.

show vlan internal usage	November 13, 2001	This command displays the VLANs that are allocated as internal VLANs for routed ports.
show vlan summary	November 13, 2001	The term "summary" in this context refers to the ability to list the number of vlans configured. The number of active vlans in a device is a parameter defined in the IEEE 802.1Q Std at Section 12.7.5, and 12.7.6.1.3.
vlan internal allocation policy	June 26, 2002	The term "internal allocation policy" refers to the allocation sequence of internal vlans used by the network element itself (not user configurable).
switchport vlan mapping	February 6, 2003	The term "mapping" in this context refers to the ability to translate the original vlan number into another as frames are received in a trunk port.

26. The following CLI commands in this litigation provide functionality relating to PVLANs (shown in chronological order based on Cisco's purported "earliest document date" for each alleged command):

Disputed "Command"	**Earliest Document Date**	**Additional Opinions**
private-vlan	January 16, 2001	The term "private vlan" is a well-known term to describe a vlan architecture that permits user isolation and restricts their communication while still been part of a single network.
private-vlan mapping	January 16, 2001	The term "mapping" refers to the

		association between a promiscuous vlan with a private vlan.
show vlan private-vlan	January 16, 2001	"show" commands come from prior legacy CLIs, as discussed elsewhere in this Report. *See above* for discussion of other comand keywords.
switchport private-vlan mapping	January 16, 2001	*See above.*